

BioPass3000

Hardware Description

Version 1.0

Feitian Technologies Co., Ltd. ("Feitian" for short) will do their best to keep the content of this document as accurate as possible. But Feitian will not take the responsibilities for any direct or indirect loss that may be caused by this document. The content of this document will be amended along with the updating of the product without notification.

Revision History:

Date	Version	Description
December 2006	1.0	1st Edition

Feitian Technologies Co., Ltd.

Software Developer's Agreement

All Products of Feitian Technologies Co., Ltd. (Feitian) including, but not limited to, evaluation copies, diskettes, CD-ROMs, hardware and documentation, and all future orders, are subject to the terms of this Agreement. If you do not agree with the terms herein, please return the evaluation package to us, postage and insurance prepaid, within seven days of their receipt, and we will reimburse you the cost of the Product, less freight and reasonable handling charges.

1. Allowable Use - You may merge and link the Software with other programs for the sole purpose of protecting those programs in accordance with the usage described in the Developer's Guide. You may make archival copies of the Software.

2. Prohibited Use - The Software or hardware or any other part of the Product may not be copied, reengineered, disassembled, decompiled, revised, enhanced or otherwise modified, except as specifically allowed in item 1. You may not reverse engineer the Software or any part of the product or attempt to discover the Software's source code. You may not use the magnetic or optical media included with the Product for the purposes of transferring or storing data that was not either an original part of the Product, or a Feitian provided enhancement or upgrade to the Product.

3. Warranty - Feitian warrants that the hardware and Software storage media are substantially free from significant defects of workmanship or materials for a time period of twelve (12) months from the date of delivery of the Product to you.

4. Breach of Warranty - In the event of breach of this warranty, Feitian's sole obligation is to replace or repair, at the discretion of Feitian, any Product free of charge. Any replaced Product becomes the property of Feitian.

Warranty claims must be made in writing to Feitian during the warranty period and within fourteen (14) days after the observation of the defect. All warranty claims must be accompanied by evidence of the defect that is deemed satisfactory by Feitian. Any Products that you return to Feitian, or a Feitian authorized distributor, must be sent with freight and insurance prepaid.

EXCEPT AS STATED ABOVE, THERE IS NO OTHER WARRANTY OR REPRESENTATION OF THE PRODUCT, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

5. Limitation of Feitian's Liability - Feitian's entire liability to you or any other party for any cause whatsoever, whether in contract or in tort, including negligence, shall not exceed the price you paid for the unit of the Product that caused the damages or are the subject of, or indirectly related to the cause of action. In no event shall Feitian be liable for any damages caused by your failure to meet your obligations, nor for any loss of data, profit or savings, or any other consequential and incidental damages, even if Feitian has been advised of the possibility of damages, or for any claim by you based on any third-party claim.

6. Termination - This Agreement shall terminate if you fail to comply with the terms herein. Items 2, 3, 4 and 5 shall survive any termination of this Agreement.

CE Attestation of Conformity

The equipment complies with the principal protection requirement of the EMC Directive (Directive 89/336/EEC relating to electromagnetic compatibility) based on a voluntary test.

This attestation applies only to the particular sample of the product and its technical documentation provided for testing and certification. The detailed test results and all standards used as well as the operation mode are listed in

Test report No.: 70407310011

Test standards: EN 55022/1998 EN 55024/1998

After preparation of the necessary technical documentation as well as the conformity declaration the CE marking as shown below can be affixed on the equipment as stipulated in Article 10.1 of the Directive. Other relevant Directives have to be observed.

FCC certificate of approval

This Device is in conformance with Part 15 of the FCC Rules and Regulations for Information Technology Equipment.

USB

This equipment is USB based.

WEEE

Dispose in separate collection.

Contents

- 1 Advantages 1
- 2 Features 2
- 3 Technical Specification 3

1 Advantages

BioPass3000 integrates advanced smartcard chip. It is the ideal device to protect user's sensitive data. Its advantages include:

- **High Performance**

Integrating dedicated high security CPU with 32-bit RISC, the device works stably under up to 100MHz frequencies. In line with a hardware multiplication coprocessor and high performance cache, the device performance achieves perfect.

- **High Security**

Integrated with hardware-based RSA algorithm, BioPass3000 is more secure than applications that only employ software-implemented RSA. Because the sensitive data is stored in the secure storage area of BioPass3000 hardware, unauthorized people cannot access the data. The data signature and encryption operation are performed inside BioPass3000. The private key is also stored inside BioPass3000 since the initial generation. These could effectively prevent hacker program attacks. In addition, the algorithms used by BioPass3000 are publicly acknowledged by the industry, widely open, and proven. The first-class chip encapsulation technique provides further security for the data that resides on the chip.

- **Easy to Use**

Using BioPass3000 does not require any additional devices. Users only need to plug BioPass3000 into the USB port of desktop computers, laptop computers, keyboards or displays. Users do not need to shut down the computer or stop any running programs. After finishing the use, users could disconnect BioPass3000 directly.

- **Low Cost**

BioPass3000 could save more cost than any other hardware-based security systems, because it does not require any additional devices. This makes BioPass3000 especially suitable for widely deployed applications. BioPass3000 could provide all the functionalities of smartcard card devices with its special advantage that no smartcard reader is required.

- **Portability**

BioPass3000 is small and light, which makes it perfectly portable. Small casing shell is manufactured by all-in-one once-forming technique. It is hard and durable with waterproof feature. Users could fit BioPass3000 conveniently on their key rings.

- **Compatibility**

BioPass3000 supports two types of most popular standard interfaces: PKCS#11 and Microsoft CryptoAPI. Any application that is compliant with these two interfaces could be integrated with BioPass3000 directly. Moreover, BioPass3000's compatibility has been optimized for many

third-party software products. Additionally, BioPass3000 integrates mass secure storage memory. It could store multiple certificates, private keys and other data. That is, multiple PKI applications could share one BioPass3000 device.

- **High Reliability**

BioPass3000 is manufactured with strict standard technique. It supports single-byte or multi-byte (up to 64) of erasing and writing. It could be erased or written to at least 500,000 times. Data stored in BioPass3000 could be retained for at least 100 years under room temperature. This effectively ensures that the sensitive data is stored securely and stably.

2 Features

- **High-performance processor chip**

BioPass3000 integrates a 32-bit secure RISC high speed SOC chip, presenting high performance, high-level security, low power dissipation and low cost features.

- **Hardware implemented encryption algorithms**

The advanced smartcard technique of BioPass3000 provides the following hardware-based encryption algorithms:

- 1) 512-bits, 1024-bits, 2048-bits RSA dissymmetrical encryption algorithms and related signature, verification functionalities
- 2) Symmetrical encryption algorithms: DES and 3DES
- 3) Digest functions: SHA-1 and MD5

Because the key encryption algorithms are implemented inside the hardware, the security of the key-pairs in encryption calculation is ensured.

- **Hardware-based RSA key-pair generator**

The BioPass3000 RSA key pairs are generated inside the hardware instantly. The grand prime numbers used to generate the key pairs are also provided by the hardware random number generator.

- **Hardware-based random number generator**

BioPass3000 integrates the hardware random number generator. This generator could be used for generating the key pairs, random access message authentication code and so on.

- **On-chip secure storage**

BioPass3000 data storage (RAM), firmware storage (ROM) and computing components are integrated within a single chip. This assures the secure storage of the data.

- **Encrypted data package**

The communications between BioPass3000 and the computer are encrypted. This design

could effectually prevent Trojan program's monitoring.

3 Technical Specification

Hardware Features	Working Voltage		5V (Powered by USB port)
	Working Current		80-150mA
	Working Temperature		5 to 40°C
	Storage Temperature		0 to 50°C
	Humidity Rating		20% to 80%
	Casing		Hard molded plastic
	Interface		Mini USB
	Fingerprint Input		Slide
	Processor		32-bit
	Memory Size		64K
	FLASH Rewrites		At least 100,000
	Data Retention		At least 100 years under room temperature
	Sensor Wear Out		100,000 times
	ESD	On pins.HBM (Human Body Model) CMOS I/O	≤2KV
		On die surface (Zapgun Air discharge)	±16KV
Software Features	Fingerprint Acquisition Time		<1s
	Fingerprint Comparing Time		<1s
	Comparing Mode		1: 1;1: N
	FRR		0.1%~0.01%
	FAR		0.01%~0.001%
	Fingerprint Storage Number		≤8
	Fingerprint Match Level		3 levels
	Fingerprint Verification Retries		No limit
	Status Indication		Two LEDs
	Certificate and Standard		PKCS # 11 v2.11, MS CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec, ISO 7816 compliant
	Built-in Security Algorithm		RSA, DES, 3DES, MD5 and SHA-1
	Chip Security		Securely encrypted data storage
	Supported OS		Windows 98 SE/Me/2000/XP/2003